Apple's Conundrum: The Immutability of Liberty vs. Security

Yaozong Ma
University of West Alabama
Livingston, Alabama

Abstract

Foundational issues of liberty versus security were questioned during the scenario involving the federal government and Apple Computer concerning an iPhone recovered from the San Bernardino shooting. A fundamental premise of this debate involved considerations of liberty and privacy versus security. In this instance, the scenario involved Apple's ability and willingness to assist the federal government to access its iPhone product. This paper provides a brief commentary regarding this scenario.

Keywords: Apple, FBI, liberty, security, national security, iPhone, terrorism

1. Introduction

Globalism presents numerous opportunities for terrorist factions to disseminate their ideologies and perform heinous actions worldwide (Doss, Guo, & Lee, 2012; Wigginton, et al., 2015). Endangerments threatening American society and its interests are commensurate with the all-hazards perspective of homeland security and emergency management that is advocated by departments of public safety among the states and the U.S. Department of Homeland Security (Doss, et al., 2016; Gallant, 2008; McElreath, et al., 2016; McElreath, et al., 2014a). Certainly, terrorism is a valid concern of both federal and state governments. Acts of terrorism have ranged from the actions of lone wolf operators to the sophistication and complexity of events sponsored by organized criminal factions (Doss, Jones, & Sumrall, 2010). After the events of 9-11, painful reminders of the dangerousness of terrorism have occurred domestically. Prominent examples include the 2009 Fort Hood massacre, the 2013 Boston Marathon bombing, and the 2015 San Bernardino shooting incident. Historically, examples range from the endeavors of the Ku Klux Klan and similar hate groups to the 1960s church bombings in Birmingham, Alabama (Doss, 2011; McElreath, et al., 2014). Although none of these events rivaled 9-11 with respect to similar, mass quantities of thousands of casualties, they involved considerations of technologies necessary for performing acts of terror. During the aftermath of the 2015 San Bernardino event, a legal dispute occurred between the Federal Bureau of Investigation (FBI) and Apple Computer. The dispute involved both technological and legal considerations of the FBI accessing an Apple iPhone. It also necessitated questioning the foundational premises of liberty versus security within American society.

In 2012, it was determined that approximately 75% of the global population had access to some type of mobile cellular telephone (Russell & Cieslik, 2012). Use of cell phones and mobile devices facilitates instantaneous communication for a variety of purposes and reasons, both benevolent and detrimental (Doss, Glover, Goza, & Wigginton, 2015). Within American society, regarding an instrumentalist philosophy and perspective, such technologies may be perceived as neutral resources that may be leveraged for either good or evil depending upon the intentions and motivations of users (Liu, et al., 2016). From a criminal context, the motivations that are catalysts for physical crime are mimicked among virtual environments (Doss, Henley, & McElreath, 2013a; Doss, Henley, & McElreath, 2013b). Given such notions, despite their philosophical neutrality as technological resources, cell phones are subject to human motivations when planning, facilitating, and perpetrating terrorist actions (Sharma, 2005).

In conjunction with increase of cell phone use over time, criminals and terrorists have crafted methods for leveraging mobile devices as tools for facilitating crime and terrorism. Cell phones may be used for conversational purposes to facilitate illegal acts or as detonation resources for terrorist bombings.

Regardless, if a cell phone (or is remaining components) is retrieved from a crime scene, one may be inclined to examine both its tangible and intangible attributes. Generally, in order for the government to conduct some type of search, a warrant must be issued per the Fourth Amendment (Yang, et al., 2016). The U.S. Constitution represents the basis for conducting searches legally. It also delineates restrictions of government powers. Essentially, it provides a basis for contemplating the foundational questions of liberty versus security within American society. Such questions debates are critical aspects of understanding the fabric of American government.

Liberty versus security is a philosophical dichotomy that has fueled many debates throughout American history. The freedoms and liberties of society were not earned without some costs. Both quantitative and qualitative costs and sacrifices were required to secure freedom and liberty. Maintaining freedom is not costless; it necessitates the continuous sacrifices of many to ensure high levels of security. Within a free society, citizens themselves must exercise the liberty and freedom of making unbiased, unfettered decisions. Basically, in order to be free, a high level of security must exist to ensure freedom. In order to ensure security, citizens must decide openly and unbiasedly to secure themselves. Thus, the immutability of freedom and security is a continuous aspect of American society throughout generations.

The federal government pursues a variety of anti-terrorism and counter-terrorism activities that involve some considerations of constitutional freedoms, liberty, privacy, and security (McElreath, et al., 2014b). After the San Bernardino shooting incident, questions of liberty versus security were not only pondered among legal environments and the justice system, but also throughout modern society. Basically, after capturing a cell phone involved with the San Bernadino shooting, various factions pondered what information it contained and how it could be used throughout legal proceedings. One could easily ponder whether any information stored within the cell phone would lead to other terrorists. One could also contemplate whether information contained within the cell phone could be used to prevent or deter future terrorist acts.

The basic premises and arguments of liberty versus security are equally important during modern times as they were during the founding of the nation (McElreath, et al., 2013). Volokh (2014) indicates that Benjamin Franklin stated, “Those who would give up essential liberty, to purchase a little temporary safety, deserve neither liberty nor safety.” Similarly, Blakely, et al., (2016) indicate that even the remainder of the founding fathers debated which was of greater importance, liberty or security? Are the historical perspectives of liberty versus security still applicable during modern times, especially with respect to terrorist acts? Given the potential of the cell phone recovered from the San Bernadino shooting to deter or prevent future terrorist acts, did Apple Computer have a moral obligation to assist federal law enforcement entities by facilitating access to its iPhone product? Essentially, given such questions, the situation involving Apple and the FBI represented a classic example of fundamental arguments involving the immutability of liberty versus security within American society.

2. Considerations of the FBI vs. Apple Scenario

In December, 2015 in San Bernardino, California, a terrorist shooting, perpetrated by Syed Rizwan Farook, resulted in the deaths of 14 individuals (Audi, Barrett, & Carlton, 2015). An Apple iPhone, possessed by Farook, was recovered during the aftermath of the shooting. This iPhone became the subject of legal and technological debates within American society. Essentially, a dimension of this debate incorporated considerations of liberty versus security.

During its investigation, some amount of enmity between the FBI and Apple occurred regarding the accessing of the iPhone. The FBI assumed that accessing the recovered iPhone would reveal connections with possible terrorists or terrorist organizations, and that knowing its contents might contribute toward deterring future terrorist incidents. Simply, Apple refused to comply initially with any federal requests for accessing the iPhone. Apple indicated an inability to access the iPhone despite having developed and produced the device. More specifically, Apple indicated that it purposefully possessed no ability to decrypt iPhone encryption (Limer, 2016).

A federal judge ordered Apple to devise some method of accessing the device (McSweeney, 2016). Providing such a resource raised various privacy, constitutionality, and hacking concerns. If an alternative method of accessing the device existed, then it was assumed that “all kinds of people” could access Apple’s iPhones worldwide (Apple, 2016). More specifically, “if the US government can demand access, the Chinese government

can do so as well; Apple exercises a soft market power to resist authoritarian demands, but it won't have a leg to stand on if the government of its own country compels access" (Apple, 2016).

Further, developing an access method would not only provide access to the recovered iPhone from the San Bernardino incident, but also for all Apple iPhones (Limer, 2016).

Apple and the FBI sought to resolve their dispute within the court system. A cornerstone of the FBI's argument was the *All Writs Act* which allowed courts to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law" (Limer, 2016). Essentially, All Writs Act provides justification and authorization for courts to craft, enact, and implement orders which compel individuals to perform acts provided that reasoning is both necessary and legal (Limer, 2016). However, the FBI dropped its suit before it was heard within the justice system because it had gained access to the iPhone. Basically, the FBI contracted another party to craft a method of accessing the iPhone.

Public debate regarding the scenario involved sentiments that pitted privacy concerns against the demands of security and safety (Blakely, et al., 2016). For many people, their iPhones may contain business, personal, and intimate types of information (Blakely, et al., 2016). Because Apple products were famous for their practically impenetrable security, providing a means of breaching security may have been viewed negatively by some market factions. Basically, Apple's competitive market position may have suffered if the company had complied with the FBI (Shinal, 2016). Essentially, Apple experienced a fiduciary obligation to its stockholders to steadfastly resist governmental attempts to force it to provide access to its products (Shinal, 2016).

Conceptually, before the third party provided access for the FBI, the scenario was quickly becoming a Catch-22 situation for Apple. If the company complied with the FBI, then it risked losing market share, market position, and profits. Its market image and reputation would be sullied, and new investors may have been reticent when considering Apple. Contrastingly, by remaining uncompliant, Apple risked contempt charges and the possibility of financial fines and sanctions. Either course of action could have resulted in losses for Apple.

3. The Terrorism Perspective

When most people are asked whether they mind giving up some privacy to help catch terrorists, Marcovici (2014) indicates that an analogous query is, "Do you want the government to engage in surveillance?" Although this question seems rather straightforward, Marcovici (2013) indicates that the true nature and intent of the question may be stated as, "Do you want the government to engage in surveillance without a warrant or probable cause?" According to Solove (2011), "Rarely does protecting privacy involve totally banning a security measure," but protecting security always tends to necessitate losses of some amounts of liberty and privacy. Thus, embroiled within the FBI vs. Apple scenario is a simple question: should privacy be sacrificed for security?

The 1993 bombing of the World Trade Center in New York, the Oklahoma City bombing, and the events of 9-11 introduced American society to the painfulness of large-scale terrorist events that may be enacted upon U.S. soil (McElreath, et al., 2014a; 2014b). During modern times, the shared roles of American law enforcement organizations, including the FBI, involves terrorism deterrence (Doss, Guo, & Lee, 2012; McElreath, et. al., 2013). Thus, the conundrum between the FBI and Apple also involved strong considerations of fulfilling modern aspects of policing missions as well as protecting national security.

Much effort, money, and time are required to effectively penetrate terrorist cells and generate useful intelligence (Doss, Sumrall, McElreath, & Jones, 2013). The iPhone retrieved from the San Bernardino shooting represented a possible opportunity to identify additional terrorists and provide intelligence that may have been critical for neutralizing future attacks. As a result, less time may have been required for penetrating terrorist networks and gaining information about future terrorist activities (Blakely, et al., 2016).

Even terrorists use cellular devices. In this instance, an iPhone was at the heart of the dispute between Apple and the FBI. The FBI wanted Apple to develop some type of "backdoor" method of accessing the captured iPhone. From the perspective of the Fourth Amendment, various concerns of warrants and electronic boundaries are pertinent regarding digital devices (Yang, et al., 2016). Although the FBI wanted to access the phone legally and insinuated emphatically that access would be used for only the captured iPhone, some raised the inevitable question of whether the FBI would use the access method for other iPhones at some point in the future thereby compromising consumer privacy and confidence (Blakely, et al., 2016; Lien & Dave, 2016).

Regardless of the consideration, something is certain: the recovered iPhone was possessed by a terrorist. Although the iPhone was possessed by a terrorist, no guarantee existed that its contents would or would not lead to the capturing of other terrorists or the thwarting of terrorist endeavors.

After all, no guarantee existed that its contents would contain any relevant data or information concerning terrorist activities or contacts. Thus, some amount of risk existed throughout the dispute.

This dispute between Apple and the FBI also introduced the potential of accessing anyone's electronic device at any time with terrorism as a justification for the search (Blakeley, et al., 2016). Thus, according to Blakely, et al., (2016, p. 3), more questions are posed: "Should the government be allowed to 'tap' into American citizen's personal devices and comb through their personal data, in the interest of national security? Or should privacy be held in higher importance over the possibility of stopping further attacks like the one in San Bernardino?" Such questions and any pondering of the Apple iPhone scenario invokes considerations of liberty and privacy versus the needs of security.

4. Concluding Comments

The notions of liberty and privacy versus security represented a foundational basis of the FBI versus Apple scenario. Apple exhibited a commitment to is stakeholders by refusing to comply with the government. Until the retrieved iPhone was accessed, the scenario was quickly become a Catch-22 scenario in which Apple would experience some type of losses regardless of its course of actions. After accessing the iPhone and making the event public knowledge, market consumers and market investors may be biased regarding their perceptions of Apple. Time will show the effects of demand for Apple's products within its competitive markets.

Accessing intelligence that may be beneficial for deterring terrorism is a paramount societal concern. Avoiding terrorist incidents (e.g., San Bernadino) may be achieved by gaining information and intelligence that contributes meaningfully to an enhanced understanding of situations. However, no guarantee existed that the recovered iPhone contained any information that would contribute to determent efforts.

Technology, in and of itself, may be viewed as a neutral tool (Liu, et al., 2016). It may either be used beneficially or malevolently per the intention and motivation of the human user (Liu, et al., 2016). This notion certainly applies to the technologies that are used by terrorists. Examining the content of the iPhone associated with the San Bernardino terrorists may yield critical data that contributed toward thwarting future incidents. Examined data may reveal additional contacts who have terrorist inclinations. As such, the iPhone has the potential of being a strong investigative resource whereby societal order may be maintained and terrorism may be deterred.

Numerous state and non-state entities, both domestic and global, desire to harm American interests via terrorism (Doss, McElreath, et al., 2014b; Doss, Jones, & Sumrall, 2010; Wigginton, et al., 2015). The San Bernardino incident is one example of how technology is integrated among terrorism scenarios. The third-party breaching of the iPhone may have an externality: by observing the breaching of Apple's security via third-party access of the recovered San Bernardino iPhone, hackers worldwide may be emboldened to increase cyber-attacks against Apple's products (Blakely, et al., 2016).

In conclusion, until its security was breached by a third-party and the case was dropped, Apple experienced a tumultuous Catch-22 situation with the federal government that involved age-old considerations of liberty and privacy versus security. At the time of this authorship, the events between Apple and the FBI continue to unfold among news media outlets. Time will eventually reveal the outcome of the scenario and its significance. Regardless of any speculation or prediction regarding the outcome, one observation is clear: given technological change and technological prevalence among modern lifestyles, contemporary society continues the debate regarding privacy and liberty versus security.

5. References

Apple. (2016). *Apple is right to challenge the FBI: But its case should only be the beginning of protecting our devices.* Retrieved from: http://www.thenation.com/article/apple-is-right-to-challenge-the-fbi/

Audi, T., Barrett, D., & Carlton, J. (2015). *San Bernardino shooting: At least 14 people killed.* Retrieved from: http://www.wsj.com/articles/active-shooter-reported-in-southern-california-1449085770

Blakely, T., Elam, K., Langley, D., Morrison, W., Robinson, D. (2016). *Apple's conundrum: Liberty vs. security and modern terrorism*. Retrieved from: www.intellectualarchive.com/getfile.php?file=9fg9UgLsfFq&orig_file=Apple-FBI%20Final%20Paper.pdf

Doss, D. (2011). *The Alabama anthology: Readings and commentaries in criminal justice*. Acton, MA: Copley Publishing.

Doss, D., Glover, W., Goza, R., & Wigginton, M. (2015). *The foundations of communication in criminal justice systems*. Boca Raton, FL: CRC Press.

Doss, D., Guo, C., & Lee, J. (2012). *The business of criminal justice: A guide for theory and practice*. Boca Raton, FL: CRC Press.

Doss, D., Henley, R., McElreath, D., Lackey, H., Jones, D., Gokaraju, B., & Sumrall, W. (2016). Homeland security education: Managerial versus nonmanagerial market perspectives of an academic program. *Journal of Education for Business, 91*(4), 203-210.

Doss, D., Henley, R., & McElreath, D. (2013a). The Arizona border with Mexico: A Pearson correlation coefficient analysis of US border crossing data versus US reported cybercrime incidents for the period of 2001-2011. *International Journal of Social Science Research, 1*(2013), 17.

Doss, D., Henley, R., & McElreath, D. (2013b). The California-Mexican border: Investigating Pearson correlation coefficient outcomes representing U.S. border crossing data versus U.S. reported cybercrime incidents during 2001-2011. *Mustang Journal of Law and Legal Studies, 4(*2013), 17-28.

Doss, D., Jones, D., & Sumrall, W. (2010, September). *A quantitative analysis of Animal Liberation Front incidents versus Earth Liberation Front incidents*. Paper presented to the annual meeting of the Southern Criminal Justice Association. Clearwater Beach, FL.

Doss, D., Sumrall, W., McElreath, D., & Jones, D. (2013). *Economic and financial analysis for criminal justice organizations*. Boca Raton, FL: CRC Press.

Gallant, B. (2008). *Essentials in emergency management: Including the all-hazards approach*. Lanham, MD: Rowman & Littlefield.

Lien, T. & Dave, P. (2016). *Apple's Tim Cook to shareholders: Taking on the FBI is the right thing to do*. Retrieved from: http://www.latimes.com/business/technology/la-fi-tn-apple-shareholder-meeting-fbi-20160226-story.html

Limer, E. (2016). *Most useful podcast ever: Why is the FBI using a 227-year-old law against Apple?* Retrieved from: http://www.popularmechanics.com/technology/a19483/what-is-the-all-writs-act-of-1789-the-225-year-old-law-the-fbi-is-using-on-apple/

Liu, M., Yang, D., He, F., Li, M., & Doss, D. (2016). *Perspectives of technology and the instrumentalist paradigm. Proceedings of the Academy of Organizational Culture, Communications, and Conflict, 21*(1), 34-38.

Marcovici, M. (2014). *You are the target: Or do you believe your government always watches the others?* Hamburg, Germany: Books on Demand.

Marcovici, M. (2013). *The surveillance society: The security vs. privacy debate*. Hamburg, Germany: Books on Demand.

McElreath, D., Doss, D., Jensen, C., Lackey, H., Wigginton, M., & Jones, D. (2016). State defense forces: Strategic resources for homeland security and emergency management. *Proceedings of the Southwest Academy of Management, 2016,* 264.

McElreath, D., Doss, D., Jensen, C., Wigginton, M., Kennedy, R., Winter, K., Mongue, R., Bounds, J., & Estis-Sumerel, J. (2013). *Introduction to law enforcement*. Boca Raton, FL: CRC Press.

McElreath, D., Doss, D., Jensen, C., Wigginton, M., Nations, R., Van Slyke, J., & Nations, J. (2014a). *Foundations of emergency management*. Dubuque, IA: Kendall-Hunt.

McElreath, D., Jensen, C., Wigginton, M., Doss, D., Nations, R., & Van Slyke, J. (2014b). *Introduction to homeland security*. (2nd ed.). Boca Raton, FL: CRC Press.

McSweeney, T. (2016). *Judge orders Apple to unlock San Bernardino killer's phone*. Retrieved from: http://www.nbcbayarea.com/on-air/as-seen-on/Judge-Orders-Apple-to-Unlock-San-Bernardino-Killer_s-Phone_Bay-Area-369072121.html

Russell, C. & Cieslik N. (2012). *Mobile phone access reaches three quarters of the planet's population*. Retrieved from: http://www.worldbank.org/en/news/press-release/2012/07/17/mobile-phone-access-reaches-three-quarters-planets-population

Sharma, D.P. (2005). *The new terrorism: Islamist international*. New Delhi, India: APH Publishing.

Shinal, J. (2016). *Smartphones don't kill*. Retrieved from: http://www.usatoday.com/story/tech/columnist/shinal/2016/02/18/apple-vs-fbi-boils-down-civil-liberties-and-shareholder-value/80548302/

Solove, D. (2011). *Why "security" keeps winning out over privacy*. Retrieved from: http://archives.californiaaviation.org/airport/msg47540.html

Volokh, E. (2014). *Liberty, safety, and Benjamin Franklin*. Retrieved from: https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/11/11/liberty-safety-and-benjamin-franklin/

Wigginton, M., Burton, R., Jensen, C., McElreath, D., Mallory, S., & Doss, D. (2015). Al-Qods force: Iran's weapon of choice to export terrorism. *Journal of Policing, Intelligence, and Counter Terrorism*, *10*(2), 153-165.

Yang, D., He, F., Li, M., Liu, M., & Doss, D. (2016). Do you have anything to declare? Considerations of the Fourth Amendment and border searches. *Proceedings of the Academy of Organizational Culture, Communications, and Conflict*, *21*(1), 66-69.